RECEIVED
CENTRAL FAX CENTER
JUL 03 2006

DILLON & YUDELL LLP

ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO:		FROM:
Examiner Jenise E. Jackson		James E. Boice, Reg. No. 44,545
ORGANIZATION:		DATE:
US Patent and Trademark Office		July 3, 2006
ART UNIT: 2131	CONFIRMATION NO.: 7195	TOTAL NO. OF PAGES INCLUDING COVER: 15
FAX NUMBER: 571-273-8300		APPLICATION SERIAL NO.: 09/847,085
ENCLOSED: Appeal Brief		ATTORNEY DOCKET NO.: RPS920000109US1

☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED
CENTRAL FAX CENTER

JUL 03 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

	§	ATTY. DOCKET NO.: **RPS920000109US1**
IN RE APPLICATION OF:	§	
	§	
DARYL CARVIS CROMER ET AL.	§	EXAMINER: ***JENISE E. JACKSON***
	§	
SERIAL NO.: **09/847,085**	§	
	§	
FILED: ***MAY 2, 2001***	§	ART UNIT: **2131**
	§	
FOR: **DATA PROCESSING SYSTEM AND METHOD FOR PASSWORD PROTECTING A BOOT DEVICE**	§	
	§	
	§	
	§	

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-16 in the above-identified application. A Notice of Appeal was filed in this case on June 20, 2006 and received in the United States Patent and Trademark Office on June 20, 2006. No appeal brief fee is believed to be required, in view of Appellants' earlier payment of the fee for filing an appeal brief on August 25, 2005, but in the event that any additional fees are required, please charge them to **Lenovo Deposit Account No. 50-3533.**

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Jane Graham *Date:* 7-3-2006 *Signature:* Jane Graham

RECEIVED
CENTRAL FAX CENTER
JUL 03 2006

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 011790, frame 0911.

RELATED APPEALS AND INTERFERENCES

There are no Appeals or Interferences known to Appellants, the Appellants' legal representative, or assignee, which would be directly affected or have a bearing on the Board's decision in the present Appeal.

STATUS OF CLAIMS

Claims 1-16 stand finally rejected by the Examiner as noted in the Final Action dated April 26, 2006. Claims 17-19 are cancelled. The rejections of Claims 1-16 are appealed.

STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final rejections that lead to this appeal.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The invention recited in Claim 1 provides a method in a data processing system for maintaining security during booting of the data processing system. According to this method, during booting of the data processing system, a boot device is interrogated for password information (Figure 2A, block 128; page 4, lines 4-5). In response to the boot device supplying a device password corresponding to that of a trusted boot device, the data processing system is booted utilizing the boot device, where the booting includes booting the data processing system utilizing the boot device without entry of a device password corresponding to that of a trusted boot device by a human user (Figure 2A, blocks 130 and 132; page 4, lines 5-10).

Appellants' Claim 4 recites a method for interrogating a plurality of boot devices for a device password by interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies a device password corresponding to that of a trusted boot device (Figure 2B, blocks 122-126; page 9, lines 13-20).

Appellants' Claim 7 recites a data processing system including a boot device (Figure 1, reference numerals 10 and 18; page 4, lines 1-10), a processor (Figure 1, reference numeral 12; page 6, line 9), and a memory coupled to the processor for communication (Figure 1, reference numeral 14; page 6, lines 10-12). The memory includes startup software that, when executed by the processor during the boot process, interrogates the boot device for a device password and, responsive to the boot device supplying a device password corresponding to that of a trusted boot device, boots the data processing system utilizing the boot device, wherein the startup software boots the data processing system utilizing the boot device without entry of a device password corresponding to that of a trusted boot device by a human user (Figure 1, reference numeral 14; page 4, lines 5-10; Figure 2A, blocks 130 and 132; page 4, lines 5-10).

Appellants' Claim 9 recites a data processing system having a plurality of boot devices, wherein startup software interrogates the plurality of boot devices for a device password in sequence according to priority order until a boot device supplies a device password corresponding to that of a trusted boot device (Figure 1, reference numeral 14; page 9, lines 13-20; Figure 2A, blocks 130 and 132; page 4, lines 5-10).

Appellants' Claim 12 recites a program product that includes a computer-usable medium (Figure 1, reference numeral 14; page 11, lines 10-15) and startup software encoded within the computer-usable medium, wherein the startup software causes a data processing system to interrogate a boot device for a device password during a boot process, and responsive to the boot device supplying a device password corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device without entry of any device password corresponding to that of a trusted boot device by a human user (Figure 2A, blocks 130 and 132; page 4, lines 5-10).

Appellants' Claim 14 recites a program product stored in a computer-readable medium for interrogating a plurality of boot devices for a device password by interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies a device

password corresponding to that of a trusted boot device (Figure 2B, blocks 122-126; page 9, lines 13-20).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. The Examiner's rejection of Appellants' Claims 1-16 under 35 U.S.C. § 112, first paragraph is to be reviewed on Appeal.

II. The Examiner's rejection of Appellants' Claims 1-16 under 35 U.S.C. § 112, second paragraph is to be reviewed on Appeal.

III. The Examiner's rejection of Appellants' Claims 1-3, 7-8, 12-13 under 35 U.S.C. § 102(b) as being anticipated by *Pearce et al.* (U.S. Patent No. 6,484,308) is to be reviewed on Appeal. The decision on this rejection will also be dispositive of the rejection of Claims 1-16 under 35 U.S.C. § 103 in view of *Pearce*.

ARGUMENTS

I. Rejection of Claims 1-16 under 35 U.S.C. § 112, first paragraph

In the Examiner's Final Action dated April 26, 2006, Claims 1-16 were rejected under 35 U.S.C. § 112, first paragraph. The Examiner asserts that the claims contain subject matter "which was not described in the specification in such a way that as to enable one skilled in the art to which it pertains . . . to make and/or use the invention".

In making the § 112, first paragraph rejection, the Examiner asserts at page 5, paragraph 19 of the Final Office Action that page 7 of the Specification indicates that the "user enters the password to determine whether or not the device is trusted." Examiner also asserts that the Specification fails to disclose that the device password is not entered by a human user as claimed in Claim 1 (viz. "wherein said booting comprises booting the data processing system utilizing the boot device without entry of any of said device password corresponding to that of a trusted boot

device by a human user"). These statements clearly reveal confusion by the Examiner between the "configuration password" entered by the user to access the BIOS configuration routine and the claimed "device password" accessed by the computer to determine if the boot device is a trusted boot device.

In the present Specification, the "configuration password" is entered by a user on receipt of a request to enter a BIOS configuration routine (Specification, page 7). The BIOS configuration routine is preferably password protected with a "configuration password" to prevent unauthorized changes to the order in which boot devices are checked for a bootable operating system at system startup.

Completely unrelated to the "configuration password" is the "device password" recited in exemplary Claim 1. The "device password" is stored on a boot device and is "utilized during startup to verify that the boot device is a trusted device from which computer system 10 is permitted to boot" (Specification, page 8, line 11). Also, still referring to the Specification, page 8, lines 13-25, the "unique device password" is in one embodiment formed by a "combination of the model and serial number of the boot device." As disclosed in the Specification, the use of model and serial numbers for the "unique device password" is preferable since the modification of such numbers is "beyond the capabilities of most individuals" and "the use of the manufacturer-specified model and serial numbers as a password offers a reasonable level of security." As further detailed in the Specification in Figure 2A, blocks 124-132 and the corresponding text on page 9, lines 20-27, the boot device is interrogated for a device password and the data processing system is booted utilizing the boot device without user entry of any device password corresponding to that of the trusted boot device.

From the forgoing, it is clear that Appellants have satisfied the requirements of enablement and written description with respect to the "device password" and other features of the claims and respectfully request that the rejections under § 112, first paragraph be reversed.

II. Rejection of Claims 1-16 under 35 U.S.C. § 112, second paragraph

At page 3, paragraph 4 of the Examiner's Final Action, Claims 1-16 were rejected under 35 U.S.C. § 112, second paragraph for allegedly failing to particularly point out and distinctly claim the subject mater which Appellants regard as the invention. More specifically, the Examiner rejects Claims 4, 9, and 14 under § 112, second paragraph, as inconsistent with the specification for reciting "interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies said device password to that of a trusted boot device". The Examiner points to page 7 of the present Specification, which discloses that the user must manually enter a configuration password in order to change the order of the boot devices, and asserts that this disclosure is inconsistent with the claims, which recite that boot devices are interrogated in sequence to determine which boot device will supply a device password information corresponding to a trusted boot device.

Again, these statements clearly indicate confusion between the "configuration password" and the "device password", disclosed in the Specification and described above in detail. Appellants utilize the term "device password" numerous times within Claims 1-16, and specifically in Claims 4, 9, and 14, to describe a password utilized to identify a boot device as a trusted boot device. For example, Claim 4 recites "interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies said *device password* corresponding to that of a trusted boot device".

Because Claims 1-16 particularly point out and distinctly claim the subject matter which Appellants regard as the invention and the claim terminology employed therein corresponds exactly with that utilized in the Specification, Appellants respectfully request that the rejections under § 112, second paragraph be reversed.

III. Rejection of Claims 1-3, 7-8, 12-13 under 35 U.S.C. § 102(b) as being anticipated by *Pearce*

In the Examiner's Final Action, Claims 1-3, 7-8, 12-13 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Pearce*. The Examiner's rejection should be reversed because *Pearce* does not teach or suggest each claimed feature. In particular, nothing in *Pearce* teaches or suggests:

> during a boot process, interrogating a boot device for password information; and
>
> in response to the boot device supplying a device password corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device . . . .

As a basis for the § 102(b) rejection, the Examiner cites col. 2, lines 13-16 of *Pearce* as disclosing "interrogating a boot device for a device password" and "in response to the boot device supplying the device password corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device". The cited passage of *Pearce* discloses that during system boot, the system management mode (SMM) software is invoked to power on the boot device to read unique drive identification information from the drive. The Examiner then asserts col. 4, lines 12-14 of *Pearce* disclose a system and method that ensures a drive inserted or used in the computer system is the drive used to boot the computer. However, the system and method disclosed in *Pearce* ensure that the drive inserted in a computer system during *system resume* after the system is placed in a suspend mode is the same drive originally used to boot the computer (col. 2, lines 28-40).

In fact, the Examiner's entire argument hinges on whether a computer system "boot" and "resume" are identical. Turning to the prior art of record, *Pearce* clearly differentiates between a "boot" and a "resume". It is well-known in the art that "boot" is a procedure of starting or restarting a computer system. This understanding is reflected in in *Pearce*, Figures 2-3, blocks 202-204 and 302-306, which the system is powered on ("computer system boot", Figure 2) the system management mode (SMM) software powers on a hard drive and reads identification information from the drive. *Pearce* contrasts "boot" with a "resume", which is the continued operation of a computer system "from a power down or suspend state" (col. 2, lines 28-30). Thus *Pearce* clearly teaches that "boot" and "resume" are different operations and are therefore not identical.

In contrast to the "resume" taught by *Pearce*, Claim 1 recites "during a boot process, interrogating a boot device for password information" and "in response to the boot device supplying a device password corresponding to that of a trusted boot device, booting the data processing system". Claim 1 clearly indicates that the actions recited in the claim occur during *the boot process*, rather than during *system resume*, as taught by *Pearce*.

In light of the preceding argument, Appellants believe that independent Claim 1, similar Claims 7 and 12 and all dependent claims are not anticipated by *Pearce*, and the Examiner's rejection under 35 U.S.C. § 102(b) should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections, and the claim language that renders the invention patentable over the combination of references. Appellants, therefore, respectfully request all of the rejections of the pending claims be reversed.

Respectfully submitted,

James E. Boice
Reg. No. 44,545
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method in a data processing system for maintaining security during booting of the data processing system, said method comprising:

during a boot process, interrogating a boot device for password information; and

in response to the boot device supplying a device password corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device, wherein said booting comprises booting the data processing system utilizing the boot device without entry of any of said device password corresponding to that of a trusted boot device by a human user.

2. The method according to Claim 1, wherein said device password includes at least a serial number of the boot device.

3. The method according to Claim 1, wherein interrogating said boot device for said device password comprises startup software interrogating the boot device.

4. The method according to Claim 1, wherein interrogating said boot devices for said device password comprises interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies said device password corresponding to that of a trusted boot device.

5. The method according to Claim 1, and further comprising:

storing a password in non-volatile storage of the data processing system; and

determining that said boot device has supplied said device password corresponding to a trusted boot device by hashing said device password supplied by the boot device and comparing the hashed device password with the stored password.

6. The method according to Claim 5, and further comprising obtaining said password by interrogating the boot device for said device password with a password-protected configuration routine.

7. Data processing system comprising:

a boot device;

a processor; and

memory coupled to said processor for communication, said memory including startup software that, when executed by said processor during a boot process, interrogates the boot device for a device password and, responsive to the boot device supplying said device password corresponding to that of a trusted boot device, boots the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said device password corresponding to that of a trusted boot device by a human user.

8. The data processing system of Claim 7, wherein said device password includes at least a serial number of the boot device.

9. The data processing system of Claim 7, said data processing system having a plurality of boot devices including the boot device, wherein said startup software interrogates said plurality of boot devices for said device password in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device.

10. The data processing system of Claim 7, and further comprising non-volatile storage that stores a password, wherein said startup software determines that said boot device has supplied said device password corresponding to a trusted boot device by hashing said device password supplied by the boot device and comparing the hashed device password with the password stored in non-volatile storage.

11. The data processing system of Claim 10, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for said device password.

12. A program product comprising:

a computer usable medium; and

startup software encoded within said computer usable medium, wherein said startup software causes a data processing system to interrogate the boot device for a device password during a boot process and, responsive to the boot device supplying said device password corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said device password corresponding to that of a trusted boot device by a human user.

13. The program product of Claim 12, wherein said device password includes at least a serial number of the boot device.

14. The program product of Claim 12, said data processing system having a plurality of boot devices including the boot device, wherein said startup software causes the data processing system to interrogate said plurality of boot devices for said device password in sequence according to a priority order until a boot device supplies said device password corresponding to that of a trusted boot device.

15. The program product of Claim 12, wherein said startup software determines that said boot device has supplied said device password corresponding to a trusted boot device by hashing said device password supplied by the boot device and comparing the hashed device password with a password stored in non-volatile storage of the data processing system.

16. The program product of Claim 15, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for the said device password.

17.-19. (canceled)

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE